UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/556,068	04/21/2000	Sai V. Allavarpu	5181-48400	6894

7590 07/13/2004

Robert C Kowert
Conley Rose and Tayon P C
P O Box 398
Austin, TX 78767-0398

EXAMINER	
PATEL, HARESH N	
ART UNIT	**PAPER NUMBER**
2154	16

DATE MAILED: 07/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/556,068	ALLAVARPU ET AL.	
	Examiner	Art Unit	
	Haresh Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-57 are presented for examination.

Specification

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "Secure access to Managed Network Objects using a configurable platform-independent CORBA gateway".

Information Disclosure Statement

3. An initialed and dated copy of Applicant's IDS form 1449, Paper No. 9, is attached to the instant Office action. Applicant needs to submit the IDS for the mentioned existing SAP concept.

Response to Arguments

4. Applicant's arguments filed 5/13/04, paper number 15, have been fully considered but they are not persuasive.

Applicant argues (1) Barker et al., U.S. patent number 6,363,421 (Hereinafter Barker) does not disclose, "a gateway that is configurable to provide object-level access control between the managers and the managed objects to send the requests to the managed objects, wherein said object-level access control is provided at the individual

object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches a gateway that is configurable to provide object-level access control between the managers (e.g., agents, col., 8, line 53 – col., 9, line 19) and the managed objects (e.g., managed objects, col., 8, line 53 – col., 9, line 19) to send the requests to the managed objects, wherein said object-level access control is provided at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63). Therefore Barker meets the claim limitation.

Applicant argues (2) Barker does not disclose, "object-level access control, wherein said object-level access control is provided at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches a gateway that is configurable to provide object-level access control between the managers (e.g., agents, col., 8, line 53 – col., 9, line 19) and the managed objects (e.g., managed objects, col., 8, line 53 – col., 9, line 19) to send the requests to the managed objects, wherein said object-level access control is provided at the individual object level so that one of the managers is granted access to one of the managed objects while being

prevented from interfacing with a different one of the managed objects (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63). Therefore Barker meets the claim limitation.

Applicant argues (3) Barker does not disclose, "determining on a managed object level, at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches a gateway that is configurable to provide object-level access control between the managers (e.g., agents, col., 8, line 53 – col., 9, line 19) and the managed objects (e.g., managed objects, col., 8, line 53 – col., 9, line 19) to send the requests to the managed objects, wherein said object-level access control is provided at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63). Therefore Barker meets the claim limitation.

Applicant argues (4) Barker does not disclose, "a gateway that is configurable to authenticate the managers to receive the events from or to send the request to the managed objects as a function of the identity of the managed object".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches a gateway that is configurable to determine on a managed object level whether or not the manager application (e.g., agent) is allowed to receive an event generated by one of plurality of managed objects (e.g., request to the managed object) or to send a request to the one of the plurality of managed objects (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63) as a function of the identity of the user of the manager application (e.g., an agent application of a client), whereby access for the manager application send the request is approved or denied for said managed object (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63). Therefore Barker meets the claim limitation.

Applicant argues (5) Barker does not disclose, "managed objects comprising one or more objects corresponding to a telephone network".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches the managed objects comprise one or more objects corresponding to a telephone network (e.g., objects of a public telephone network (PSTN), col. 3, lines 47 – 54, figure 1A, remote management of a telecommunication network elements, title, FIG. 1A is a functional block diagram of an embodiment of the network element management system in which the management computer, or work station, is employed to control, or manage, a

plurality of network elements of a telecommunication network through a public switched telephone network (PSTN); FIG. 1B is a functional block diagram of an embodiment of the network element management system in which the management computer, a work station, is employed to control, or manage, a plurality of network elements of a telecommunications network through a computer internet; FIG. 1C is a functional block diagram of an embodiment of the network element management system in which the management computer, or work station, is employed to control, or manage, a plurality of network elements of a telecommunication network through a local area network, col., 2, line 49 – col., 3, line 40). Therefore Barker meets the claim limitation.

Applicant argues (6) Barker does not disclose, "security audit trails".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches the gateway (server) is configurable to provide security audit trails (e.g., client registration and filtering, auditing, col., 17, line 27 – col., 18, line 67). Therefore Barker meets the claim limitation.

Applicant argues (7) Barker does not disclose, "a gateway providing access to a logging service".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches the gateway (server) providing security audit trails comprises the gateway providing access to a logging service (e.g., use of storage devices to store filtered, audited and events information, col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53). Therefore Barker meets the claim limitation.

Applicant argues (8) Barker does not disclose, "the requests are converted from the IDL to a platform-specific format (Portable Management Interface (PMI)) prior to delivery to the managed object".

The examiner disagrees in response to applicant's arguments. Barker clearly teaches that the requests are converted from the interface definition language to a platform-specific format prior to delivery to the managed objects, the requests are converted from the interface definition language to a Portable Management Interface (PMI) format prior to delivery to the managed objects (e.g., conversion from the IDL to a network element specific protocol, The specific protocol used for communication with the network element is specified by the service object. The SNMP protocol is used for communication between service objects associated with the AP and the AP network element. Other managed object classes could be added that utilize a different protocol and encapsulate that knowledge in the managed object class, hence any protocol, like PMI can be supported, col., 21, line 46 – col., 22, line 59). Therefore Barker meets the claim limitation.

Response to Amendment

5. Applicant's amendment to the claims 1-57 (paper number 15) have been considered. Note: Even though the same cited reference is used for rejection, mapping of the cited reference teachings for the claimed limitations have been changed to overcome the applicant's amendment to the claims.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-57, are rejected under 35 U.S.C. 102(e) as being anticipated by Barker et al. U.S. patent number 6,363,421.

8. As per claims 1, 20 and 39, Barker teaches the following:

a network management method / a carrier medium/ system comprising (e.g., a management computer is connected to an element management system server through a special communication link including a computer internet, col. 1, lines 27-30),

a gateway (e.g., an element management server, col.1, lines 27-30) which is coupled to a plurality of managed objects (e.g. plurality of network elements coupled to the element management server through the computer internet, e.g., col. 1, lines 29-36) and which is configured to deliver events generated by the managed objects to one or more managers (e.g., the element management server is provided with application processor specific events and command acknowledgements, col. 1, lines 63-65) or to deliver requests generated by the managers to one or more of the managed objects (e.g., the element management server is provided with application processor specific events and command acknowledgements, col. 1, lines 63-65); and

a platform-independent interface to the gateway (e.g., use of CORBA to serve as the IPC for functions residing on the server to eliminate any platform-specific IPC implementation, also use of Internet Inter-Object Protocol, col. 4, lines 37-55), wherein the gateway is configurable to communicate with the managers through the platform-independent interface to deliver the events or requests (e.g., the element management server is provided with application processor specific events and command acknowledgements, col. 1, lines 63-65),

wherein the gateway is configurable to provide object-level access control between the managers (e.g., agents, col., 8, line 53 – col., 9, line 19) and the managed objects (e.g., managed objects, col., 8, line 53 – col., 9, line 19) to send the requests to the managed objects, wherein said object-level access control is provided at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63),

delivering the event to the manager application or the request to the managed object if the manager access is approved (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63),

determine on a managed object level whether or not the manager application (e.g., agent) is allowed to receive an event generated by one of plurality of managed objects

(e.g., request to the managed object) or to send a request to the one of the plurality of managed objects (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63) as a function of the identity of the user of the manager application (e.g., an agent application of a client), whereby access for the manager application send the request is approved or denied for said managed object (e.g., concept of the use of a naming service that provides individual object level access control so that an agent is granted access to an object on the network to support IIOP protocol, col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63).

9. As per claims 2-4, 21-23 and 40-42, Barker teaches the following:

the gateway is configurable to determine whether each of the managers is authorized to communicate with each of the managed objects (e.g., the server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 8, lines 31-54),

the gateway is configurable to authenticate the managers to receive the events from or to send the requests to the managed objects as a function of the identity of the managed object objects (e.g., the server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 8, lines 31-54),

the gateway is configurable to authenticate the managers to receive the events or send the requests as a function of user IDs entered by users of the managers objects (e.g., the server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 8, lines 31-54).

10. As per claims 5, 24 and 43, Barker teaches the following:

the events or requests are delivered by the gateway through the platform-independent interface according to Internet Inter-Object Protocol (IIOP) (e.g., use of IIOP protocol, col. 9, lines 15-19).

11. As per claims 6-7, 25-26 and 44-45, Barker teaches the following:

the platform-independent interface to the gateway is expressed in an interface definition language (e.g., use of interface description language (IDL), col. 39, lines 1-15, figure 15), and wherein the interface definition language comprises a language for defining interfaces to the managed objects across a plurality of platforms and across a plurality of programming languages (e.g., IDL is used to describe any resource or service a server component wants to expose to its clients without regard to its implementation language or operating system, col. 39, lines 1-15, figure 15),

the interface definition language comprises OMG IDL (e.g., use of object management group (OMG) IDL, col. 7, lines 1-30).

12. As per claims 8-9, 27-28 and 46-47, Barker teaches the following:

the managed objects comprise one or more objects corresponding to a telephone network, the managed objects comprise an object corresponding to a telecommunications device (e.g., objects of a public telephone network (PSTN), col. 3, lines 47 – 54, figure 1A, remote management of a telecommunication network elements, title, FIG. 1A is a functional block diagram of an embodiment of the network element management system in which the management computer, or work station, is employed to control, or manage, a plurality of network elements of a telecommunication network through a public switched telephone network (PSTN); FIG. 1B is a functional block diagram of an embodiment of the network element management system in which the management computer, a work station, is employed to control, or manage, a plurality of network elements of a telecommunications network through a computer internet; FIG. 1C is a functional block diagram of an embodiment of the network element management system in which the management computer, or work station, is employed to control, or manage, a plurality of network elements of a telecommunication network through a local area network, col., 2, line 49 – col., 3, line 40).

13. As per claims 10-15, 29-34 and 48-53, Barker teaches the following:

the gateway (server) is configurable to provide security audit trails (e.g., client registration and filtering, auditing, col., 17, line 27 – col., 18, line 67),

the gateway (server) providing security audit trails comprises the gateway providing access to a logging service (e.g., use of storage devices to store filtered,

audited and events information, col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53),

the logging service is operable to log an ID of a user that sends each request (e.g., ID of an agent application associated with a particular user request, col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53),

the logging service is operable to log an ID of the managed object that is the source of each event or the target of each request (e.g., request/status/event containing the managed object identifier, col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53),

the logging service is operable to log a time (time of a request/status/event) at which each event or request is generated (e.g., the time when a request/status/event is generated, col., 11, lines 18 – 60, col. 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53, col., 31, lines 15 – col., 43, col., 39, line 24 – col., 40, line 29, col., 23, line 55 – col., 24, line 10),

the logging service is operable to log a time at which each event or request is delivered (e.g., the time when a request/status/event is delivered, col., 11, lines 18 – 60, col. 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53, col., 31, lines 15 – col., 43, col., 39, line 24 – col., 40, line 29, col., 23, line 55 – col., 24, line 10).

14. As per claims 16-17, 35-36 and 54-55, Barker teaches the following:

the requests comprise a query for information concerning one of the managed objects (e.g., each managed object service class must implement the managed object

interface, which defines configuration and status services like viewconfig, used to obtain configuration information for all network elements, col. 40, lines 27-38),

the requests comprise a command to set one or more parameters of one of the managed objects (e.g., each managed object service class must implement the managed object interface, which defines configuration and status services like viewconfig, used to obtain configuration information for all network elements, col. 40, lines 27-38).

15. As per claims 18-19, 37-38 and 56-57, Barker teaches the following:

the requests are converted from the interface definition language to a platform-specific format prior to delivery to the managed objects, the requests are converted from the interface definition language to a Portable Management Interface (PMI) format prior to delivery to the managed objects (e.g., conversion from the IDL to a network element specific protocol, The specific protocol used for communication with the network element is specified by the service object. The SNMP protocol is used for communication between service objects associated with the AP and the AP network element. Other managed object classes could be added that utilize a different protocol and encapsulate that knowledge in the managed object class, hence any protocol, like PMI can be supported, col., 21, line 46 – col., 22, line 59).

Conclusion

16. Examiner makes a very clear note that the rational of the applicant's invention has been clearly taught by the cited reference. Applicant's invention does contain few minor

additional matters that facilitate the concepts of the applicant's invention. However, the additional minor matters are well known in the art.

17. The concept of the use of a CORBA gateway for object level access control, including the use of Service Access Point (SAP) with insertion of the user name in the request message, is well known in the prior art. The prior art made of record (Forms PTO-892) and not relied upon is considered pertinent to applicant's disclosure.

Apte, US 2004/0111730 A1, June 10, 2004, also discloses use of CORBA Server and the object level access control.

Feuerman, 6,529,947, "Managing transiently connected network clients", discloses use of name service to provide object level access control over the network among objects.

Applicant submitted, IDS, paper number 9, N. Lynch et. al., "Web Enabled TMN Manager", clearly discloses use of CORBA with the existing TMN devices for object level access control.

Taylor et al, 6,256,676, "Agent-adapter architecture for use in enterprise application integration systems", discloses use of object level access control for variety of objects.

Bowman-Amuah, 6,640,249, "Presentation services patterns in a netcentric environment", discloses use of CORBA server, naming service, security audit trails, etc.

Houlding, 6,75,771, "System and method for delivering web services using common object request broker architecture", discloses use of CORBA naming service for object level access control among objects.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Haresh Patel whose telephone number is (703) 605-5234. The examiner can normally be reached on Monday, Tuesday, Thursday and Friday from 10:00 am to 8:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee, can be reached at (703) 305-8498.

The appropriate fax phone number for the organization where this application or proceeding is assigned is (703) 306-5404.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Haresh Patel

June 15, 2004

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100